

**REMARKS**

Applicants respectfully traverse the rejections of the pending claims. Applicants wish to immediately respond to the lack of written description concern raised regarding the limitation of "revocation file" in claim 36. Applicants respectfully note that this concern is raised without addressing the arguments noted in the April 22, 2004 response that specifically addressed this very question, which Applicants repeat as follows: Authentication methods in digital rights management (DRM) schemes are known. Indeed, as set forth in the U.S. Patent Application 2003/0105718 by Hurtado, [previously] cited against the cancelled claims, it is known to use digital certificates, see paragraph 194 [of that reference]. Content providers provide digital certificates to content users so that they become authorized to access protected content. For example, a user at a host device such as a personal computer may obtain a digital certificate that is then provided to a storage engine controlling access to protected content stored on a storage medium. The authentication process comprises verifying a digital signature provided by the content provider that is contained within the digital certificate. Once the signature is authorized, the user is authenticated and may proceed to access the protected content.

However, because digital signatures involve the use, typically, of private/public key cryptography that may become compromised, there is another layer of protection commonly available in conventional DRM schemes. That layer would be the revocation process, which follows authentication. In other words, even though a user may possess a valid certificate, if that user is identified by a revocation list, the user is denied access to

the protected content. The Hurtado discloses a conventional revocation scheme at, for example, paragraph 368, wherein Hurtado states:

The End-User Player Application 195 stores a copy of the Clearinghouse's 105 certificate revocation list on the End-User Device(s) 109. Whenever a revocation list is received, the End-User Player Application 195 replaces its local copy if the new one is more up to date. Revocation lists includes a version number or a time stamp (or both) in order to determine which list is the most recent.

As is conventional, this Hurtado revocation scheme follows authentication. It is performed as an initial handshaking routine between the host device and the storage engine.

In contrast to the conventional revocation scheme disclosed in Hurtado [and also the currently cited Nonaka reference], the present invention provides a file-by-file revocation scheme. It is not performed immediately following authentication but instead is much more granular in that it precedes any file request by the host device. Consider, for example, pages 32 and 33 of the disclosure. As set forth by the Applicants, in their revocation scheme, each file may have its own associated revocation list, see for example, lines 21 through 23 on page 32. As such, this type of revocation would not be performed immediately after authentication – a user may or may not desire access to any given file on the storage medium. Not only do the Applicants provide greater granularity and control, the revocation itself is more adaptable in that the associated revocation list with a given file comprises a set of rules for evaluating fields in the digital certificate against data in the revocation list, see for example lines 24 through 28 on page 32.

Although the disclosure discussed above plainly supports “revocation file” in that one need not have ipso facto, word-for-word, support for claim terms, Applicants have amended claim 36 to use “revocation list” instead of “revocation file.” In addition, the

preamble of claim 36 has been amended to reflect the granular, file-by-file revocation scheme being claimed.

The Nonaka reference adds nothing further to the previously distinguished (and successfully traversed) Hurtado reference. In that regard, Applicants note that they are indeed arguing about specific claimed limitations with regard to their file-by-file revocation scheme.

**Applicants respectfully stress the following: Nonaka makes absolutely no suggestion or teaching for the limitation of “reading a revocation list associated with the file” with regard to a file request as set forth in claim 36.** In that regard, Applicants submit that it would be helpful to review the revocation scheme disclosed in the Nonaka publication (2003/0046238). As discussed with regard Figure 1 in ¶179, a user home network 103 includes a “network device” 160<sub>1</sub> (which will be referred to hereinafter as the “network device SAM”) and audio-visual machines 160<sub>2</sub> through 160<sub>4</sub>. All of these networked devices include a “secure application module” (SAM) (the audio-visual machines will be referred to hereinafter as the “audio-visual SAMs”). The network device receives a “secure container” file 104 from a content provider 101. To gain access to the encrypted content within the secure container, the network device interfaces with an “EMD service center” 102. The secure container may be received over the Internet or may be received offline in a storage medium as shown in Figures 11 – 16.

Any revocation discussed in Nonaka would be with regard to the entire secure container and not to specific files within the secure container. Instead, as described in ¶671 of Nonaka, revocation is between the SAMs. Specifically, “in performing

communication between the SAMs, each SAM checks the revocation list for whether the corresponding SAM has become invalid, in which case, the communication therebetween is discontinued.” Although Nonaka never explicitly addresses the issue, it is evident that this revocation check occurs during the “mutual authentication” of the corresponding SAMs as discussed, for example, in ¶516, which concerns the playback of content in one of the audio/visual SAMs as governed by the network device SAM.

Given this context, the amendment to claim 36 will now be addressed. In general, it is known in digital rights management (DRM) to use certificates that are presented between devices to establish authenticity. Because there is the possibility of a device obtaining a valid certificate through improper means, DRM schemes often provide for a revocation step following authentication of the certificate. In other words, a device may present a valid certificate but may be revoked because of its improper actions. Thus, DRM schemes often include the step of checking a device’s identity subsequent to authentication of a valid certificate against a revocation list. If the device is indicated as revoked, access is cut off despite the possession of a valid certificate.

Once a device has been established as authentic and not revoked, conventional DRM schemes may proceed to respond to file requests, etc. However, Applicants’ DRM scheme is different. As set forth, for example, on page 30, line 3 through page 35, line 21 with regard to Figures 7A-7F, Applicants granular, file-by-file revocation scheme proceeds subsequent to establishment of a secure session. As shown in Figures 7A and 7B, a host presents a certificate to the storage engine. If the certificate is authentic, the storage engine transmits a secure session key to the host to establish a secure session. During this secure session, various file requests may be issued by the host as discussed

with regard to Figures 7C-7F. This file requests are checked on a file-by-file basis.

Thus, a host may be revoked with regard to a first file but not with regard to a second file.

Such revocation flexibility is unavailable in conventional DRM schemes.

Claim 36 reflects this advantageous flexibility as discussed above.

Thus, revocation is a file-by-file decision during the secure session recited in claim 36.

A host may be authenticated and be allowed to read a given file during a secure session

but not another. Given this context, it becomes clear that the SAMs in Nonaka do not

represent a "host device" and a "storage engine" as recited in claim 36. Specifically,

Nonaka never teaches or suggests the following: subsequent to authentication and

establishment of a secure session, responding to a file request by checking for revocation

as recited in claim 36. Instead, the Nonaka revocation (to the extent that this revocation

is disclosed) is simply the all-or-nothing revocation of the prior art. In particular, note

that the file request (the internal interrupt to play content as set forth in ¶514) occurs first.

Subsequent to this request, there is mutual authentication and exchange of a session key

as set forth in ¶516. Accordingly, the pending claims are allowable over the Nonaka

publication.

With regard to the §112, second paragraph rejection of claim 36, Applicants

respond that have set forth the concrete act of "denying the file request," which is not a

statement of intended use. If the objection goes to the conditional nature of this act, in

that it is performed only "if the application of the at least one rule provides a failing

result" test is satisfied, Applicants note that they have successfully traversed the same

issue in their response of November 16, 2004, which Applicants repeat as follows:

Consider the usual flowchart – it will have often have decision blocks containing a question having a yes or no answer. If you answer yes, you go down one branch in the flowchart whereas if you answer no you go down another branch. This type of conditional branching is quite definite and very commonly used in claims. Indeed, Applicants note that Richard reference (USP 5,922,074) cited in the 11/3/04 office action is absolutely rife with the use of “if” statements in its claims. For example, consider claim 1 of this patent, which recites the step of “verifying that said digital certificate is valid.” Clearly, there are two results obtainable in response to such a step: either the certificate is verified as valid or it is not. Thus, the claim then recites the step of “retrieving, if the digital certificate is valid, an access control rule...” This conditional statement is not indefinite at all: it follows definitely from the previous act.

More fundamentally, Applicants note that the statutes, caselaw, and MPEP § 2173 set forth absolutely no such rule (that “if” renders claims indefinite). Here, claim 36 is directed to a method of revoking a host device on a file-by-file basis. This revocation is responsive to the act of “applying the at least one rule on the data in the revocation list and the associated data in the certificate.” There can only be two outcomes with respect to revocation: the host is revoked or the host is not revoked. Thus, claim 36 recites the act of “if the application of the at least one rule provides a failing result, denying the file request.” Similarly, claim 40 sets forth the act of “if the application of the at least one rule provides a successful result, granting the file request.” In other words, that host is not revoked should the application of the at least one rule provide a successful result. There is no indefiniteness to such conditional language – it is just as definite as that used in claim 1 of USP 5,922,074. Accordingly, because this conditional language is definite

and because the use of conditional language is not proscribed by the statutes, caselaw, or by the MPEP, Applicants respectfully request that the indefiniteness rejections be withdrawn.

### CONCLUSION

For the above reasons, pending Claims 36-40 are in condition for allowance and allowance of the application is hereby solicited. If the Examiner has any questions or concerns, a telephone call to the undersigned at (949) 752-7040 is welcomed and encouraged.

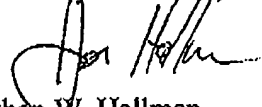
#### Certification of Facsimile Transmission

I hereby certify that this paper is being facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

  
Jonathan Hallman

November 28, 2006  
Date of Signature

Respectfully submitted,

  
Jonathan W. Hallman  
Attorney for Applicants  
Reg. No. 42,622